The University of Scranton

Division of Information Technology

Executive Sponsor:
Chief Information Officer

Responsible Office:
Information Security

Issued: 9/2020
Revised:
Reviewed:

Password Standard

I. Policy Statement
This policy establishes the requirements for creating strong passwords, best practices for protecting those passwords, and the frequency passwords should be changed.

II. Reason for Policy
Passwords are a critical component of information security, serving to protect user accounts. Not utilizing strong passwords can result in the compromise of the University's systems, data, or network.

III. Entities Affected By This Policy
All users of University IT resources who have a user account are governed by this policy. This includes students, faculty, staff, graduate teaching assistants, work study students, and all third parties.

IV. Website Address for this Policy
www.scranton.edu/information-technology/policies.shtml

V. Related Documents, Forms, and Tools

Related documents include but are not limited to:

Acceptable Use of Information Technology Resources Policy

Information Security Policy

VI. Contacts
For policy clarification and interpretation, contact the Associate Vice President for Information Technology/CIO at 570-941-6185. For legal advice and interpretation of law, please contact the Office of General Counsel at 570-941-6213.

VII. Definitions
N/A

VIII. Responsibilities
All users of University information systems are required to formulate a strong password using the requirements below when either assigned a user ID /access for the first time as a new member of the University community, and/or during prompted password reset periods. Assistance and guidance for the new user or password reset process is available at the Technology Support Center.

1. The following strength standards must be followed in setting new passwords:
    a. Passwords must be at least 9 characters and no more than 15 characters.
    b. Passwords must contain:

i. At least one number (e.g., 0-9)
ii. At least one alphabetic character (a-z)

c. Passwords should contain:
   i. A mix of upper- and lower-case characters
   ii. One or more special characters from this list: * + - / : ? _
d. Passwords should not contain:
   i. The following special characters: @ $ & ( ) , < > ‘ ; = # % “ ! or a space.
   ii. Personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
   iii. The user’s username or RoyalID
   iv. The reverse of the username or RoyalID
   v. The user’s email address
   vi. Dictionary words, including proper names
   vii. Common keyboard sequences or patterns, such as aaabbb, qwerty, zyxwvuts, or 123321
   viii. Any version of “password”, “Scranton”, “Royals”, etc.

2. Consider using a passphrase instead of a password.
3. A password cannot be reused within 60 days of changing it.
4. Passwords should be changed at least every 180 days.
5. In the event a password is forgotten, users can reset the password through the My.Scranton portal.
6. To avoid unauthorized access to University IT resources, passwords should be protected by following these guidelines:
   a. Use the password only to access University services (i.e., don’t use the same password for non-University services, like banking or external email).
   b. Do not share the password with anyone.
   c. Do not collect passwords from others.
   d. Avoid writing your password down.
   e. Do not share the answers to challenge questions you have selected as part of forgotten password/password reset processes.
   f. Do not allow browsers to store any passwords.
   g. Avoid emailing passwords, but if you must, encrypt the email.
7. A user who suspects that his or her password has been compromised must change it immediately using the My.Scranton portal or with the assistance of the Technology Support Center (570-941-4357), and must report the incident to the Information Security Office (infosec@scranton.edu).

IX. Procedures

Violations of this policy result in suspension or loss of the violator’s use privileges, with respect to Institutional Data and University owned Information Systems. Violators shall be subject to the regular disciplinary processes and procedures of the University that apply to students, faculty, staff, graduate teaching assistants, work study students, and all third parties.

X. Appendix A